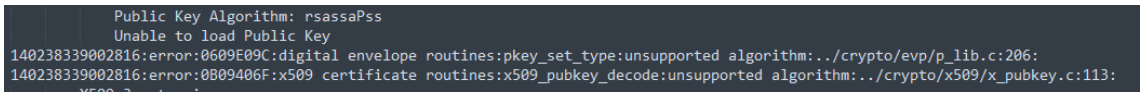
Pergunta 4

Como somos o grupo 11 o país correspondente é a Alemanha e as entidades certificadoras selecionadas foram: *D-Trust GmbH* e *Deutscher Sparkassen Verlag GmbH*;

D-Trust GmbH

Para a construção da hash foi utilizado o SHA512, que nos parece bastante razoável utilizar uma hash de 512 bits e parece-nos "future-proof" considerando o poder computacional atual e previsto para os próximos anos. Em relação ao algoritmo de chave pública/privada encontramos algumas dificuldades uma vez que o openssl não foi capaz de o identificar corretamente.



Pelo que percebemos foi utilizado uma variação do RSA, o "rsassaPss". Esta variação é pouco conhecida e talvez por essa razão o openssl não o suporta e não foi capaz de extrair a chave pública corretamente.

Deutscher Sparkassen Verlag GmbH

Para a hash foi utilizado o SHA1, que já foi considerado "oficialmente inseguro" , visto já terem sido alvo de vários ataques bem sucedidos e de já serem conhecidas colisões. A nossa recomendação neste caso é que fosse utilizado o novo algoritmo para hash SHA3. Em relação ao algoritmo de chave privada/pública está a ser utilizado o RSA, com um tamanho de chave pública de 2048 bits, parecendo-nos bastante seguro.